

iTrusCA 2.0 系统

技术白皮书

天威诚信数字认证中心

北京天威诚信电子商务服务有限公司

iTruschina Co., Ltd

北京天威诚信电子商务服务有限公司

总部地址：北京市海淀区知春路6号锦秋国际大厦A座14层1401

总部邮编：100088

总部电话：010-82800896

总部传真：010-82800636

网址：https://www.itrus.com.cn

天威诚信数据中心:

地址：北京市海淀区东北旺西路 8 号中关村软件园 21 号楼启明星辰大厦

电话：010-82825567

传真：010-82825615

客户服务热线：800-810-1303

电子信箱：support@itrus.com.cn

华东营销中心:

地址：上海市普陀区曹杨路 450 号绿地和创大厦 1702 室

邮编：200063

电话：021-33608128

传真：021-33608110

华南营销中心：

地址：深圳科技园南区软件园 T3-A108

邮编：518057

电话：0755-26745995/96/97

传真：0755-26745996

西南分公司：

地址：成都市人民南路天府大道高新孵化园 8 号楼 2020 室

邮编：610041

电话：028--85335287/97

传真：028--85335287-616

目　录

1　前言 1
2　PKI/CA技术简介 2
2.1　什么是公钥基础设施（PKI） 2
2.2　什么是认证中心（CA） 2
2.3　完整的PKI/CA体系框架 2
3　iTrusCA2.0 系统概述 4
3.1　简介 4
3.2　系统架构与组成 4
4　iTrusCA2.0 系统功能介绍 6
4.1　证书处理 6
4.2　证书生命周期管理 6
4.3　证书服务 6
4.4　系统管理功能 6
4.5　账号管理 7
4.6　策略管理 7
4.7　统计、审计与日志 7
4.8　密钥管理 7
5　技术标准和技术规范 8
6　iTrusCA2.0 系统特点 9
7　系统运行环境 10
7.1　系统模块组成 10
7.2　系统网络架构（最小配置建议） 11
7.3　系统运行软硬件环境（最小配置建议） 11

1 前言

今年 4 月 1 日起《电子签名法》开始正式施行，这是一部被誉为中国信息化领域的第一部法律。它的实施为电子商务和电子政务的发展打造了一个良好的法律环境。《电子签名法》通过确立电子签名法律效力、规范电子签名行为在法律制度上保障了网上应用系统安全，是中国信息化立法的一个突破。

《电子签名法》的出台将很好解决了网络环境中的身份认证、信息传输机密性和完整性以及抗抵赖性等系列问题。使用电子签名之后，按照目前的技术手段，其加密技术极难破解，无法伪造，因而黑客无法破译。因此我们可以说《电子签名法》的实施将大大增强网上应用系统的安全性，提高企业运作效率。

PKI/CA（PKI：Public Key Infrastructure，公钥基础设施；CA：Certification Authority，认证中心）是《电子签名法》最为认可、技术最成熟和使用最普遍的一种技术手段，所有这些电子签名应用后的优越功能，势必会给企业信息化安全建设带来新一轮的高潮。

概括起来，网上应用系统所面临的安全问题有：

- 身份认证与授权：在网上交互过程中，如何对双方进行认证，以保证交互双方身份的正确性；
- 保密性：敏感信息在网络传输以及存储过程必须保证其保密性，不允许被非法第三方窃取；
- 完整性：敏感信息在网络传输过程中必须防止被恶意窜改，在信息接收时需要对信息完整性做校验；
- 抗抵赖：对敏感操作必须保证具有抗抵赖性，对敏感操作要保留证据，一旦发生纠纷，可以根据保留的证据来提供仲裁依据。

对于这些安全问题，最有效的解决方案是建立在一种叫做公开密钥技术基础上的 PKI/CA。

2 PKI/CA 技术简介

2.1 什么是公钥基础设施（PKI）

公钥基础设施（Public Key Infrastructure，PKI），从字面上去理解，就是利用公开密钥理论和技术建立的提供安全服务的在线基础设施。所谓基础设施，就是在某个大环境下普遍适用的系统和准则。在现实生活中一个简单的例子是电力系统，它提供的服务是电能，我们可以把电灯、电视、电吹风机等看成是电力系统这个基础设施的一些应用。公钥基础设施则是希望从技术上解决网上身份认证、电子信息的完整性和不可抵赖性等安全问题，为网络应用（如浏览器、电子邮件、电子交易）提供可靠的安全服务。

公钥系统中的用户都有一对相关的密钥，其中一个密钥加密的信息只能被相应的另一个密钥解密。用户保存其中一个密钥作为私钥，而把另一个密钥与拥有者的信息捆绑后公开发布为公钥.这样，人们可以用别人的公钥加密信息，而只有私钥持有者才能读懂该信息；还可以用自己的私钥签名信息，其他人利用公钥就可鉴别信息发送者的身份。

2.2 什么是认证中心（CA）

公钥加密需要解决一个问题：加密信息的发送者需要认定公钥确实是接收者的，如果他用第三者的公钥去加密，他希望的接收者无法解密该信息，而拥有私钥的第三者却可以做到。这实际上就涉及到应用公钥技术的关键：如何确认某个人真正拥有的公钥。

在 PKI 中，为了确保用户的身份及他所持有密钥的正确匹配，公开密钥系统需要一个值得信赖而且独立的第三方机构充当认证中心（Certification Authority，CA），来确认声称拥有公开密钥的人的真正身份。就象公安局发放的身份证一样，认证中心发放一个叫“数字证书”的身份证明。这个数字证书包含了用户身份的部分信息及用户所持有的公开密钥。像公安局对身份证盖章一样，认证中心利用本身的私钥为数字证书加盖上数字签名。

任何想发放自己公钥的用户，可以去认证中心申请自己的证书。认证中心在鉴定该人的真实身份后，颁发包含用户公钥的数字证书。其他用户只要能验证证书是真实的，并且信任颁发证书的认证中心，就可以确认用户的公钥。

认证中心是公钥基础设施的核心，就象电力基础设施中的发电厂。有了大家信任的认证中心，用户才能放心方便的使用公钥技术带来的安全服务。

2.3 完整的PKI/CA 体系框架

PKI/CA 负责生成、管理、存储、分发和吊销公钥证书，完整的 PKI/CA 体系不仅仅指软硬件系统，还应该是软件、硬件、人员、策略、流程和法律协议等的总和，完整的 PKI/CA 体系如下图所示：


系统硬件
法律协议
责任规则
安全策略
系统软件
服务对象
网络环境
PKI
管理原则
物理安全
系统构架
技术标准
运作制度
技术实现
密钥管理
认证规则
信任关系

3 iTrusCA2.0 系统概述

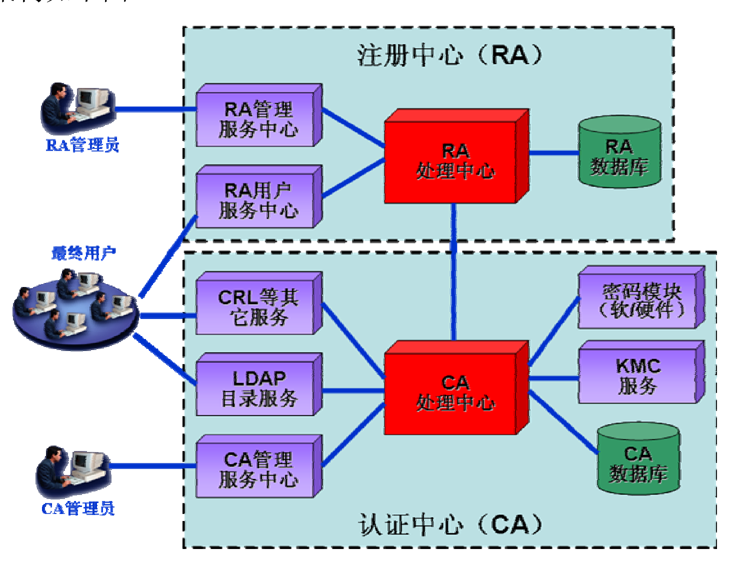
3.1 简介

天威诚信 iTrusCA2.0 系统是参照国际领先的 PKI/CA 系统的设计思想，继承了国际领先的 PKI/CA 系统的成熟性、先进性、安全可靠及可扩展性，自主开发的、享有完全自主知识产权的数字证书管理系统。

iTrusCA2.0 系统设计的证书容量为百万级，根据需要可以进行扩展；系统支持软件加密和硬件加密两种方式；根据需要并进行配置后，可以发放各种类型的证书；系统具有完善的功能；能够满足自主建立 PKI/CA 平台的需求。

3.2 系统架构与组成

iTrusCA2.0 系统架构如下图：



如图所示，iTrusCA2.0 系统由最终用户、RA 管理员、CA 管理员、注册中心（RA）、认证中心（CA）等构成：

(1) 认证中心（CA）：认证中心（CA）是 PKI/CA 平台的核心，提供证书服务和管理的主要功能。认证中心（CA）分为前台、后台两部分，前台主要用于与外界的交互及进行信息转换，后台完成核心的操作。CA 前台提供的服务包括：证书目录服务（LDAP）、证书吊销表服务（CRL）、证书状态查询服务（OCSP）和时戳服务等；后台的服务包括：证书管理服务、系统管理服务、证书数据库、签名服务器和密码设备等。

(2) 注册中心（RA）：注册中心（RA）是 PKI/CA 平台的前台，为最终用户提供用户证书服务功能，为 RA 管理员提供 RA 管理服务功能。为最终用户提供的证书服务功能包括：证书申请、证书查找、证书下载、证书吊销和证书更新等。RA 管理员可以完成用户证书批准、用户证书吊销和 RA 策略设置等功能。RA 与最终用户之间使用服务端鉴别的 SSL 协议

通信，RA 与 CA 之间使用专门的安全通信协议。

(3) CA 管理员：CA 管理员负责对 CA 系统、RA 帐户及 RA 管理员进行管理。第一和第二个 CA 管理员的证书在系统初始化时产生，其他的 CA 管理员由两个 CA 管理员共同批准。CA 管理员负责对各 RA 帐户进行管理，包括 RA 帐户批准、创建和修改，以及对 RA 管理员证书的批准和吊销等管理。整个系统的策略配置，以及操作审计日志也由 CA 管理员管理。

(4) RA 管理员：RA 管理员主要处理 RA 系统的管理以及 RA 端的用户请求，包括批准证书、废止证书、拒绝请求、通知用户下载和管理员维护等处理。RA 管理员使用 RA 管理员证书访问管理站点进行管理。

(5) 最终用户：最终用户是 CA 系统的最终服务对象。通过 CA 系统，最终用户申请获得数字证书，并进行各种各样的证书管理工作。这些最终用户证书管理功能包括：证书申请、证书下载、证书查询和证书更新等。除了证书管理，最终用户还是证书使用者，相关的应用使用最终用户客户端密码模块存放的证书和私钥，来完成签名或加密等处理。

4 iTrusCA2.0 系统功能介绍

天威诚信 iTrusCA2.0 系统提供完善的功能，包括：证书处理功能、证书生命周期管理功能、证书服务功能、系统管理功能、帐号管理功能、策略管理功能、统计审计与日志功能和密钥管理功能等。

4.1 证书处理

系统使用 XML 描述 X509 证书格式和内容，可根据需要配置签发证书的证书类别、语言种类、证书格式和证书内容。

- ✓ 支持证书版本，支持 x509 v1/v3；
- ✓ 多语种，支持用户 DN 采用各语种模式（目前实现中英文）；
- ✓ 支持自定义证书扩展项，支持三个扩展项；
- ✓ 根据需要可配置签发各种用途证书，包括：
- ✓ 邮件证书
- ✓ 个人身份证书
- ✓ 企业证书
- ✓ 服务器证书
- ✓ VPN 证书
- ✓ 代码签名证书

4.2 证书生命周期管理

- ✓ 证书申请
- ✓ 证书批准
- ✓ 证书查询
- ✓ 证书下载
- ✓ 证书吊销
- ✓ 证书更新

4.3 证书服务

CRL 证书吊销列表服务，配置指定 RA 的 CRL 下载地点及 CRL 发布时间；

LDAP 目录查询服务，支持电子邮件、用户名和组织名的任意组合查询及模糊查询。

4.4 系统管理功能

- ✓ RA 管理员管理，包括初始化 RA 管理员申请、增加 RA 管理员、删除 RA 管理员；
- ✓ CA 管理员管理，包括初始化 CA 管理员申请、后续 CA 管理员证书申请、吊销 CA 管理员证

书。

4.5 账号管理

- ✓ 个人账号管理，包括注册信息，证书信息等管理；
- ✓ RA 账号管理，包括 RA 账号申请、批准、吊销、额外管理员证书申请等。

4.6 策略管理

证书策略配置管理，高度灵活和可扩展的配置 CA 所签发证书的有效期、证书主题、证书扩展、证书版本、密钥长度、证书类型等方面；

- ✓ RA 策略配置管理，包括语言、联系方法、证书类型、是否发布到 LDAP 等；
- ✓ CA 策略配置管理，包括证书 DN 重用性检查、CA 别名设置等。

4.7 统计、审计与日志

- ✓ 统计各 CA、RA 账号证书颁发情况；
- ✓ 记录所有 RA 与 CA 的操作日志；
- ✓ 对所有操作人员的操作行为进行审计。

4.8 密钥管理

- ✓ CA 密钥产生和存储（包括根 CA 和所有子 CA 密钥，支持软件与硬件）；
- ✓ CA 密钥管理、归档与备份；
- ✓ CA 证书的产生和管理；
- ✓ 用户密钥的管理服务（KMC 服务）。

5 技术标准和技术规范

iTrusCA2.0 采用了下述标准和规范：

操作系统： Windows 2000/2003， Linux， Solaris， HP-UX、AIX

加密硬件：山大、天融信、卫士通， SZD12， SZD24

数据库：Oracle， Sybase， DB2， SQL Server， MySQL

目录服务：iPlanet Directory Server， OpenLDAP

采用规范：《证书认证系统密码及其相关安全技术规范》

加密算法：RSA， SSF33， SHA1

6 iTrusCA2.0 系统特点

iTrusCA2.0 系统是天威诚信自主开发的、享有完全自主知识产权的数字证书管理系统，系统拥有如下特点。

(1) 符合国密办规定，支持双证书、双中心，即加密证书/签名证书和 CA 认证中心/密钥管理中心；

(2) 证书类型多样性及灵活配置：系统能够提供各种证书的签发功能，根据客户需要可以进行灵活配置，包括：邮件证书、个人身份证书、企业证书、服务器证书、代码签名证书和 VPN 证书等。

(3) 灵活的认证体系配置：系统支持树状的客户私有的认证体系，支持多级 CA，支持交叉认证，支持虚拟（托管）CA。

(4) 注册机关（RA）建设方式多样化：系统支持管理不同类型证书的 RA，单个 RA 也可以管理多种类型的证书；系统支持单级 RA，也支持多级 RA；RA 界面风格可定制。

(5) 高安全性和可靠性：使用高强度密码保护密钥，支持加密机、智能卡、USB Key 等硬件设备，用户关键信息散列保存，以防遗失。

(6) 高扩展性：根据客户需要，对系统进行配置和扩展，能够发放各种类型的证书；系统支持多级 CA，支持交叉 CA；系统支持多级 RA。

(7) 多语言支持：后台业务数据处理使用 UTF－8 格式，支持多语言数据。因此，系统能过通过配置实现对不同语言证书的签发，包括支持中英文证书。

(8) 易于部署与使用：系统所有用户、管理员界面都是 B/S 模式，CA/RA 策略配置和定制以及用户证书管理等都是通过浏览器进行，并具有详细的操作说明。

(9) 高兼容性

- ✓ 跨平台设计，支持 Linux/Unix/Windows 主流操作系统；
- ✓ 支持多种加密设备：软加密库、山大加密机和天融信加密机等；
- ✓ 支持多种数据库：Oracle 和 SQL server 等；
- ✓ 支持多种证书存储介质：硬盘、USB Key 和智能卡等。

(10) 系统冗余设计，可靠性高、稳定性好符合国际和行业标准：系统在设计中遵循了相应的国际和工业标准，包括 X.509 标准、PKCS 系列标准、IETF 的 PKIX 工作组制定的 PKI 相关 RFC 标准，以及 HTTP、SSL、LDAP 等互联网通讯协议等。严格遵循这些标准，使得系统具有很好的开放性，能够与各种应用结合，成为真正的安全基础设施。

7 系统运行环境

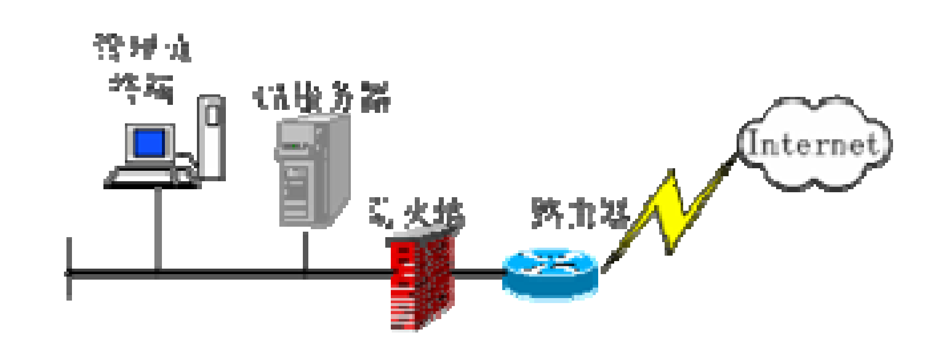
iTrusCA2.0 系统的系统模块、系统网络拓扑架构和系统运行环境如下：

7.1 系统模块组成

iTrusCA2.0 系统			
模块		功能	备注：
基本功能模块	RA 基本模块包括： RA 用户服务模块 RA 证书处理模块 RA 管理模块 RA 数据库系统 CA 基本模块包括： 业务通讯模块 RA 帐户注册模块 CRL 发布模块 证书服务处理模块 CA 管理模块 密码模块（软/硬件，缺省为软件加密模块）	● 面向最终用户提供证书管理服务； ● 面向 RA 管理员提供 RA 管理服务； ● 面向 CA 管理员提供 CA 管理服务； ● 证书吊销列表（CRL）服务； ● 证书发布和 LDAP 目录查询服务。	
可选功能模块	邮件证书模块	● 具有签发邮件证书的功能	
	个人身份证书模块	● 具有签发个人身份证书的功能	
	企业证书模块	● 具有签发企业证书的功能	
	服务器证书模块	● 具有签发服务器证书的功能	
	VPN 证书模块	● 具有签发 VPN 设备证书的功能	
	代码签名证书模块	● 具有签发代码签名证书的功能	
	OCSP 模块	● 建立 OCSP 服务	
	时间戳模块	● 提供数字时间戳服务	
	KMC 服务模块	● 建设 KMC，提供集中密钥管理服务	

7.2 系统网络架构（最小配置建议）

iTrusCA2.0 系统最小配置（证书数量在 1000 以内）建议安装在一台服务器上，建设的系统网络架构如下图所示：



7.3 系统运行软硬件环境（最小配置建议）

根据建议的系统网络架构（最小配置），系统运行软硬件环境需求如下：

系统运行环境				
硬件环境				
模块	数量	平台	配置	备注：
CA 服务器	1	PC Server	硬件： P4 1.5GHz， 512M RAM， HD 15G 软件： Windows 2000 Server，IIS 5.0 及以上 iPlanet Directory Server 4.1	安装 iTrusCA2.0 系统的所有功能模块 注 1 注 2
管理员终端	1	PC	硬件： P4 1G 128M RAM 软件： Windows 2000 Professional IE5.0 及以上浏览器	
软件环境				

数据库软件	1	SQL Server 2000	
Web 服务器软件	1	IIS 5.0 及以上服务器软件	

注 1：硬件与软件平台的版本为参考，系统升级不另通知。

注 2：密码模块缺省配置为软件加密模块，可以使用硬件密码机。